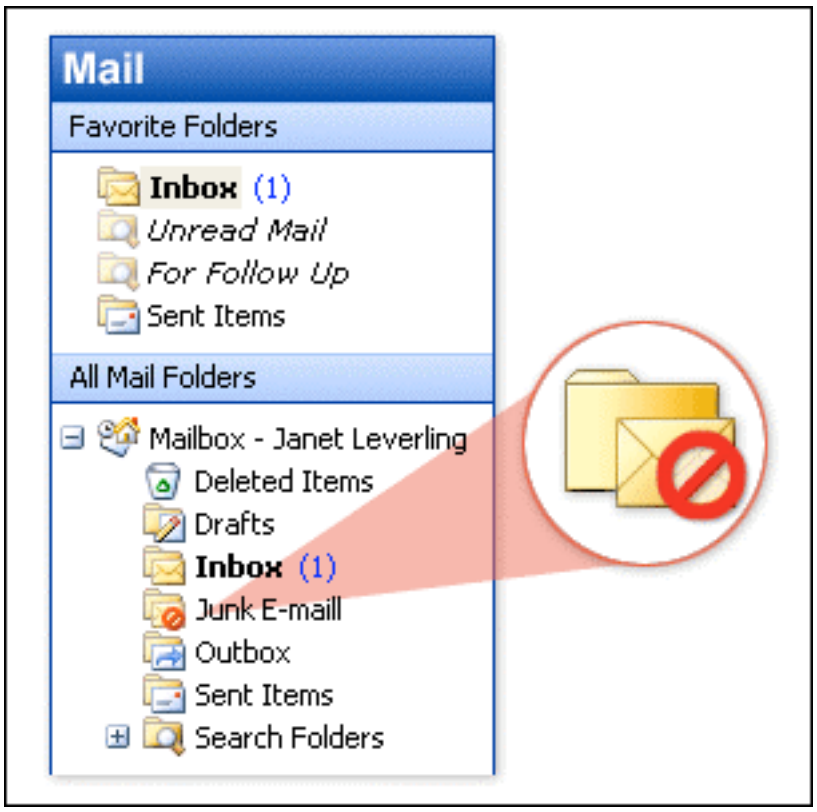
ADVS Email Filtering

OUTLOOK 2003 JUNK Folder/Filter

Microsoft Outlook 2003 reviews each email received. Email determined to be SPAM is moved to the "Junk E-mail" folder. The Outlook Junk filter/control is independent of the Firewall SPAM controls. The following is the official user guide to using the Microsoft Outlook 2003 Junk/SPAM control. It is very important to fully understand the Outlook Junk/SPAM control before configuring your Outlook Junk filter. Please print this document and become familiar with its contents before making changes in Outlook.

Outlook treats a message as junk because of several factors, including the time it was sent, the sender, the names on its “To line”, and its content. The process is complex, but you always have ultimate control over how much filtering is done.



If the Junk E-Mail filter deems a message to be Junk, the message is moved to the Junk E-mail folder, which you see in the Navigation Pane.
But what if the filter makes a mistake? That's the benefit of having messages go into the Junk E-mail folder.
You can delete a single message in the Junk E-mail folder by selecting it and clicking the delete button or you can empty the entire folder, right-click it in the Navigation Pane, and click “Empty Junk E-mail”.

To open the Junk E-mail Options dialog box do the following:

- From the Tools menu select Options
- Under the Preferences tab under E-mail, click on the Junk E-mail button

You can fine-tune the Junk E-mail Filter with the Junk E-mail Options dialog box.

- Use these tabs to view and modify the Safe Senders, Safe Recipients, and Blocked Senders lists.
- These options adjust the level of protection. Your choice here determines the filtering applied to incoming messages.

Adjust the level of protection that the filter provides. You would do this by using the dialog box shown here. If you selected the High option, Outlook would consider incoming messages very suspiciously. If you selected the No Automatic Filtering option, only messages from people you'd specified would be blocked

Edit the Junk E-mail filter lists

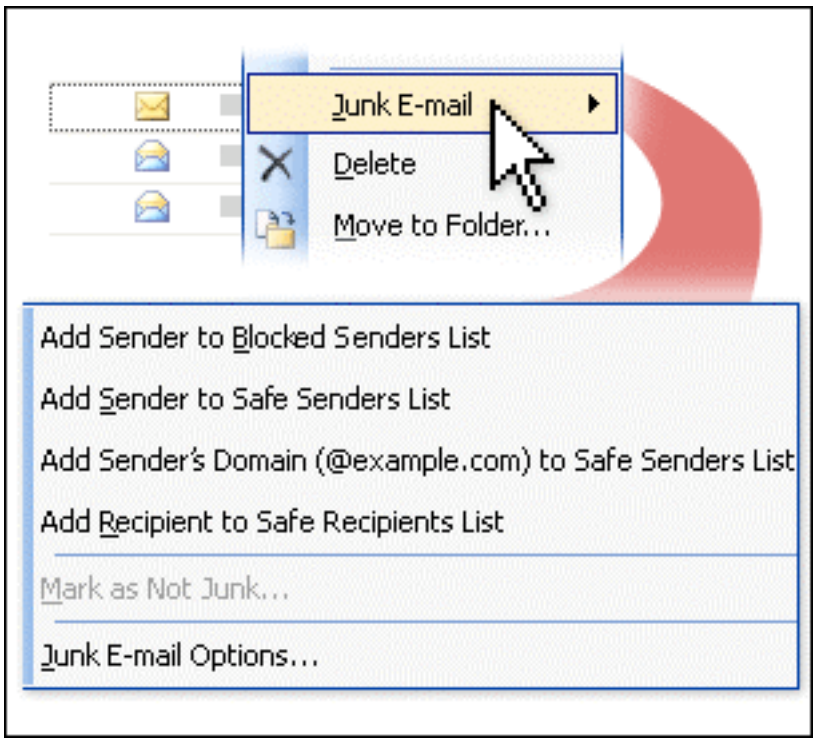
- On the Tools menu, Click Options
- On the Preferences tab, under e-mail click Junk E-mail
- Click the Safe Senders, Sage Recipients, or Blocked Senders tab
- Do one of the following:

Change a domain name or e-mail address

- In the list, click the domain name or e-mail address you want to change.
- Click Edit
- Enter the new test in the Enter an e-mail address or Internet domain name to be added to the list box.

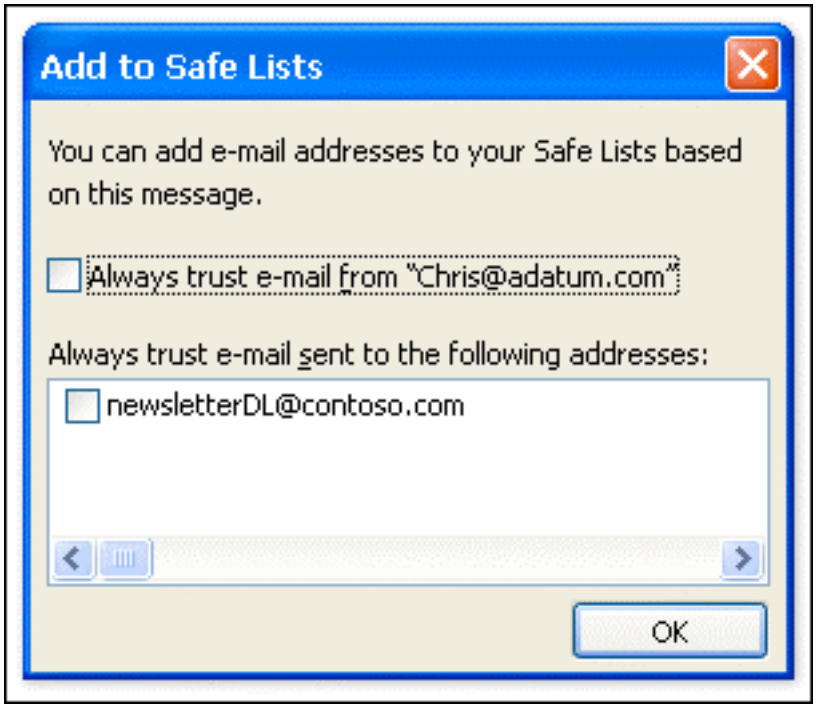
Remove a domain name or e-mail address

- In the list, click the domain name or e-mail address you want to delete
- Click Remove



Most likely, your Safe and Blocked lists will evolve as you receive e-mail. Outlook lets you add names to these lists straight from messages in your Inbox. You could do this by right-clicking the message, clicking Junk E-mail, and choosing commands from the shortcut menu shown in the picture. You could remove names, or add them, from the Junk E-mail Options dialog box.

E-mail messages from people on the Safe Senders List or to people on the Safe Recipients List will automatically be allowed into your Inbox. E-mail messages from people on the Blocked Senders List will be blocked from your Inbox and sent to the Junk E-mail folder.



Safe Senders List:

A sender is any e-mail address that you see in the From line of a message. If you add an e-mail address to the Safe Senders List, any message from that name will be considered safe.

Some junk mailers change the sender name automatically for every message. If you add full e-mail addresses to your Blocked list, such as amy@hotmail.com, you may still see spam the next day from amy@hotmail.com.

The part of an e-mail address after the @ sign is called the domain. It identifies the computer or network on the Internet that was used to send the message. You'll be glad to know that by using a domain name in your blocked list, you can, for example, avoid all messages from "adatum.com."

On the other hand, if "@adatum.com" means mail to or from someone you know, you don't want any of those messages to go to the Junk E-mail folder. Including the domain name on your Safe lists will allow all messages with that domain to pass directly to your Inbox.

What can you do to prevent Junk-mail from your inbox?

Watch out for check boxes that are already selected:

- When you buy things online, companies sometimes add a check box (already selected!) to indicate that it is fine to sell or give your e-mail address to other businesses (third parties). Clear the check box so that your e-mail address won't be shared.

Don't reply to spam:

- Don't reply even to unsubscribe unless you know and trust the sender. Answering spam just confirms that your e-mail address is live.
- If a company uses e-mail messages to ask for personal information, don't respond by sending a message Most legitimate companies will not ask for personal information in e-mail. Be suspicious if they do. It could be a spoofed e-mail message meant to look like a legitimate one. This tactic is known as "phishing" because, as the name implies, the spam is used as a means to "fish" for your credentials, such as your account number and passwords that are necessary to access and manipulate your financial accounts. If the spam is from a company that you do business with — for example, your credit card company — call the company, but don't use a phone number provided on the e-mail. Use a number that you find yourself, either through directory assistance, a bank statement, a bill, or other source. If it is a legitimate request, the telephone operator should be able to help you.

Don't contribute to a charity based on a request in e-mail:

- Unfortunately, some spammers prey on your good will. If you receive an appeal from a charity, treat it as spam. If it is a charity that you want to support, find their number elsewhere and call them to find out how you can make a contribution.

Don't forward chain e-mail messages:

- Besides causing more traffic over the line, forwarding a chain e-mail message might be furthering a hoax, and you lose control over who sees your e-mail address.

ADVS Email Filtering Explanation

ADVS email SPAM/Junk filtering is done at two levels, first by the firewall and second by Outlook 2003 upon delivery.

FIREWALL

The firewall scans every incoming email with an application called SpamAssassin. SpamAssassin thoroughly examines each email's source, servers used, subnet/country location, and content. All details gathered from an email message are checked against public databases containing SPAM information. Each email message is scored accordingly. SPAM scores can range from 0 or less to over 60. Each email header (normally not visible to you) is then modified to include the SpamAssassin score.

Emails scoring 7 or higher result in the subject of the message being "tagged" with *** SPAM *** followed by the original email subject text.

The firewall is set to capture (not deliver) emails with a score of 10 or greater.

Emails scoring 7 or 8 will get delivered and will be tagged with *** SPAM ***. The ADVS employee can then review any tagged messages to determine if the message should be deleted or is legitimate.

True SPAM is illegal which means it is unsolicited or contains a phishing type scam. Phishing scams attempt to direct the recipient to a false web site to enter private account information so a hacker can then use that information to access your legitimate account.

Most "mass marketing" email will get tagged due to the message characteristics even though it technically is HAM (legitimate) email. HAM or legitimate mass market email will honor all opt out requests and will not sell their email lists. Legitimate mass email lists get email addresses strictly form the user at their request such as when you register on a web page.

Email sent from "free" email services such as Hotmail and Yahoo will usually also score high enough to get tagged. This is due to hackers using these types of accounts to conduct unauthorized/illegal SPAM activity.

Some ISPs and organizations or agencies that have not appropriately setup their email system and or fail to control spamming will result in email from these domains being tagged with *** SPAM ***. Unfortunately if a hacker successfully gains control and uses a legitimate email server for spamming, email from this server will be subject to additional scoring due to the actions of the spammers. Email from Earthlink, ASU, and even other state or military agencies has been tagged with *** SPAM *** in the past.

Delivering Emails tagged with *** SPAM *** that score 7 or 8 will allow the ADVS employee to determine if they want to read the email or delete it. Please use the opt out option of any mass market email you have received and no longer want to be on the list.